35.G2561

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#5

In re Application of:	)	
	:	Examiner: Unknown
KEIICHI IWAMURA	)	
	:	Group Art Unit: Unknown
Appln. No.: 09/537,877	)	
	:	
Filed: March 29, 2000	)	
	:	
For: INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING APPARATUS, AND COMPUTER-READABLE RECORDING MEDIUM	)	July 31, 2000

Commissioner For Patents
Washington, D.C. 20231

CLAIM TO PRIORITY

Sir:

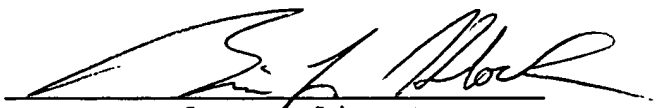
Applicant hereby claims priority under the International Convention and all rights to which he is entitled under 35 U.S.C. § 119 based upon the following Japanese Priority Application:

11-093000, filed March 31, 1999.

A certified copy of the priority document is enclosed.

Applicant's undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should be directed to our below-listed address.

Respectfully submitted,



Attorney for Applicant

Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

BLK\fdb:cmv

CFG 2561 US
09/537,817
Keiichi Iwamura
3-29-00

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　３月３１日

出願番号
Application Number: 平成１１年特許願第０９３０００号

出願人
Applicant (s): キヤノン株式会社

２０００年　４月２１日

特許庁長官
Commissioner,
Patent Office
近藤隆彦

特許庁長官印

出証番号　出証特２０００－３０２９１４８

【書類名】　特許願

【整理番号】　3927111

【提出日】　平成11年 3月31日

【あて先】　特許庁長官殿

【国際特許分類】　H04K 1/00

【発明の名称】　情報処理システム、情報処理装置及びコンピュータ読み取り可能な記憶媒体

【請求項の数】　30

【発明者】

【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

【氏名】　岩村　恵市

【特許出願人】

【識別番号】　000001007

【氏名又は名称】　キヤノン株式会社

【代理人】

【識別番号】　100090273

【弁理士】

【氏名又は名称】　國分　孝悦

【電話番号】　03-3590-8901

【手数料の表示】

【予納台帳番号】　035493

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705348

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　情報処理システム、情報処理装置及びコンピュータ読み取り可能な記憶媒体

【特許請求の範囲】

【請求項１】　複数の情報処理装置がネットワーク上に接続された情報処理システムにおいて、

上記複数の情報処理装置のうちの少なくとも一つの情報処理装置に、

入力情報に対して第１の付加情報を第１の付加方法により耐性強く付加する第１の付加手段と、

上記入力情報に対して第２の付加情報を第２の付加方法により付加する第２の付加手段とを設けたことを特徴とする情報処理システム。

【請求項２】　上記第１の付加手段を有する情報処理装置と第２の付加手段を有する情報処理装置とが異なる場合に、上記各情報処理装置間で通信を行う通信手段を設けたことを特徴とする請求項１記載の情報処理システム。

【請求項３】　上記第１の付加情報は、上記第２の付加方法を特定することのできる情報であることを特徴とする請求項１記載の情報処理システム。

【請求項４】　上記第１の付加情報は、上記ネットワーク上の各情報処理装置を特定することのできる情報であることを特徴とする請求項１記載の情報処理システム。

【請求項５】　上記第２の付加方法は、第１の付加方法と異なることを特徴とする請求項１記載の情報処理システム。

【請求項６】　上記第２の付加情報は、上記入力情報の品質を劣化させることが少ない又は人間が知覚しにくい情報であることを特徴とする請求項１記載の情報処理システム。

【請求項７】　上記第２の付加情報は、上記第１の付加情報より多いことを特徴とする請求項１記載の情報処理システム。

【請求項８】　上記第２の付加方法は、第１の付加方法と同じことを特徴とする請求項１記載の情報処理システム。

【請求項９】　上記第１の付加方法は、各情報処理装置に共通の秘密情報を

用いることを特徴とする請求項１記載の情報処理システム。

【請求項１０】　上記秘密情報は、上記第１の付加情報の位置又は第１の付加情報に対する変化量であることを特徴とする請求項９記載の情報処理システム。

【請求項１１】　上記情報処理装置は、上記第１、第２の付加情報が付加された入力情報からその付加情報を抽出する第１、第２の抽出手段を有することを特徴とする請求項１記載の情報処理システム。

【請求項１２】　上記第１又は第２の付加手段を用いて上記入力情報に付加情報を付加する前にそれに対応する上記第１又は第２の抽出手段を用いて上記入力情報に付加されたそれ以前の付加情報の検査を行うことを特徴とする請求項１記載の情報処理システム。

【請求項１３】　複数の情報処理装置がネットワーク上に接続された情報処理システムにおいて、

上記複数の情報処理装置のうちの少なくとも一つの情報処理装置に、入力情報から第１の付加情報を第１の抽出方法により抽出する第１の抽出手段と、

上記抽出された第１の付加情報から第２の抽出方法を特定し、この第２の抽出方法により上記入力情報から第２の付加情報を抽出する第２の抽出手段とを設けたことを特徴とする情報処理システム。

【請求項１４】　上記第１の抽出手段を有する上記情報処理装置と上記第２の抽出手段を有する情報処理装置とが異なる場合に、上記各情報処理装置間で通信を行う通信手段を設けたことを特徴とする請求項１３記載の情報処理システム。

【請求項１５】　上記第１又は第２の付加情報のみ抽出されたときは、上記入力情報に対して攻撃があったものと判定し、第１、第２の付加情報ともに抽出されないときは、上記入力情報には付加情報がないものと判定する判定手段を上記情報処理装置に設けたことを特徴とする請求項１３記載の情報処理システム。

【請求項１６】　入力情報に対して第１の付加情報を第１の付加方法により耐性強く付加する第１の付加手段と、

上記入力情報に対して第２の付加情報を第２の付加方法により付加する第２の

付加手段とを設けたことを特徴とする情報処理装置。

【請求項１７】　上記第１の付加情報は、上記第２の付加方法を特定することのできる情報であることを特徴とする請求項１６記載の情報処理装置。

【請求項１８】　上記第１の付加情報は、ネットワーク上の各情報処理装置を特定することのできる情報であることを特徴とする請求項１６記載の情報処理装置。

【請求項１９】　上記第２の付加方法は、第１の付加方法と異なることを特徴とする請求項１６記載の情報処理装置。

【請求項２０】　上記第２の付加情報は、上記入力情報の品質を劣化させることの少ない又は人間が知覚しにくい情報であることを特徴とする請求項１６記載の情報処理装置。

【請求項２１】　上記第２の付加情報は、上記第１の付加情報より多いことを特徴とする請求項１６記載の情報処理装置。

【請求項２２】　上記第２の付加方法は、第１の付加方法と同じことを特徴とする請求項１６記載の情報処理装置。

【請求項２３】　上記第１の付加方法は、ネットワーク上の各情報処理装置に共通の秘密情報を用いることを特徴とする請求項１６記載の情報処理装置。

【請求項２４】　上記秘密情報は、上記第１の付加情報の位置又は第１の付加情報に対する変化量であることを特徴とする請求項２３記載の情報処理装置。

【請求項２５】　上記第１、第２の付加情報が付加された入力情報からその付加情報を抽出する第１、第２の抽出手段を有することを特徴とする請求項１６記載の情報処理装置。

【請求項２６】　上記第１又は第２の付加手段を用いて上記入力情報に付加情報を付加する前にそれに対応する上記第１又は第２の抽出手段を用いて上記入力情報に付加されたそれ以前の付加情報の検査を行うことを特徴とする請求項２５記載の情報処理装置。

【請求項２７】　入力情報に対して第１の付加情報を第１の抽出方法により抽出する第１の抽出手段と、

第２の付加情報を第２の抽出方法により抽出する第２の抽出手段とを設けたこ

とを特徴とする情報処理装置。

【請求項２８】　上記第１又は第２の付加情報のみ抽出されたときは、上記入力情報に対して攻撃があったものと判定し、第１、第２の付加情報ともに抽出されないときは、上記入力情報には付加情報がないものと判定する判定手段を設けたことを特徴とする請求項２７記載の情報処理装置。

【請求項２９】　入力情報に対して第１の付加情報を耐性強く付加する第１の付加処理と、

上記入力情報に対して第２の付加情報を付加する第２の付加処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項３０】　入力情報から第１の付加情報を抽出する第１の抽出処理と、

上記抽出された第１の付加情報から抽出方法を特定する特定処理と、

上記特定された抽出方法により上記入力情報から第２の付加情報を抽出する第２の抽出処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル画像データやディジタル音声データ等の入力情報に電子透かしを情報埋め込むことにより著作権の保護、偽造防止、各種情報記録等を行う場合に用いて好適な情報処理システム、情報処理装置及びそれらに用いられるコンピュータ読み取り可能な記憶媒体に関するものである。

【０００２】

【従来の技術】

近年のコンピュータ及びネットワークの発達は著しく、文字データ、画像データ、音声データ等、多種の情報がコンピュータ内、ネットワーク内で扱われるようになってきている。このようなデータはディジタルデータであるために、同質のデータの複製を容易に作成できる環境にある。このため、こうしたデータの著作権を保護するために、画像データや音声データの中に著作権情報や利用者情報

を電子透かし情報（以下、単に電子透かしという）として埋め込む処理がなされる場合が多い。

【０００３】

ここで、電子透かしとは、画像データや音声データに所定の処理を施すことによって、これらのデータの中に、人間の視覚や聴覚では認識できないような別の情報を密かに埋め込む技術である。この電子透かしを画像データや音声データから抽出することにより、著作権情報や利用者情報、及び識別情報などを得ることができ、不正コピーを追跡することが可能となる。

【０００４】

このような電子透かしに求められる第１の条件は、埋め込まれた情報が知覚できない、即ち、元のディジタル情報の品質を劣化させることが少ないように埋め込めることである（品質）。

第２の条件は、ディジタル情報の中に埋め込まれた情報が残り続ける、即ち、データ圧縮やフィルタ処理のような編集や攻撃を受けても、埋め込まれた情報が失われないことである（耐性）。

第３の条件は、用途に応じて埋め込める情報の情報量が選択できることである（情報量）。

【０００５】

電子透かしに求められるこれらの条件は、一般的に互いにトレードオフの関係にある。例えば、耐性の強い電子透かしを実現しようとした場合、比較的大きな品質劣化が生じ、また埋め込む情報量が少なくなることが多い。

【０００６】

また、多値の静止画像を例にとると、電子透かしを埋め込む方法として、空間領域に埋め込む方式と周波数領域に埋め込む方法との二つに大きく分類でき、下記のような種々の方法が知られている。

空間領域に埋め込む方式の例としては、パッチワークによるものとしてＩＢＭの方式（W. Bender, D. Gruhl, N. Morimoto, Techniques for Data Hiding, ”proceedings of the SPIE, San Jose CA, USA, February

１９９５）やG. B. Rhoads, W. Linn:“Steganography method employing embedded”, USP Patent Number5, ６３６, ２９２などが挙げられる。

【０００７】

また、周波数領域に埋め込む方式の例としては、離散コサイン変換を利用するものとして、ＮＴＴの方式（中村、小川、高嶋、”ディジタル画像の著作権保護のための周波数領域における電子透かし方式”、ＳＣＩＳ’９７－２６Ａ，１９９７年１月）の他に、離散フーリエ変換を利用するものとして、防衛大の方式（大西、岡、松井、”ＰＮ系列による画像への透かし署名法”、ＳＣＩＳ’９７２６Ｂ，１９９７年１月）や、離散ウェーブレット変換を利用するものとして、三菱、九大の方式（石塚、坂井、櫻井、”ウェーブレット変換を用いた電子透かし技術の安全性と信頼性に関する実験的考察”、ＳＣＩＳ’９７－２６Ｄ，１９９７年１月）及び松下の方式（”ウェーブレット変換に基づくディジタル・ウォーターマークー画像圧縮、変換処理に対するロバスト性についてー”、井上、宮崎、山本、桂、ＳＣＩＳ’９８－３．２．Ａ，１９９８年１月）などが挙げられる。

【０００８】

以上のような方式は、電子透かしの埋め込み処理と抽出処理とは一対一に対応しており、基本的に互換性はない。また、一般に空間領域に埋め込む手法は、品質劣化は少ないが耐性が弱く、周波数変換を用いる手法は、品質劣化は比較的大きいが耐性が強いと言われており、耐性は強いが埋め込める情報量が少ない手法や、品質は良いが耐性の弱い手法など方式毎にその特徴は異なる。

【０００９】

さらに、これらの電子透かしは埋め込まれている情報を守るために、そのアルゴリズムや埋め込み位置や変化量などを示す情報（以後、鍵という）は秘密にされる場合が多い。これは、アルゴリズムや埋め込み位置等を解析することによって電子透かしを除去しようとする故意の攻撃に対する耐性を強くするためである。

【００１０】

一方、効率的に著作権を保護するために、電子透かしの抽出等を行い不正コピーが行われていないかどうかを検査する監視機関を設けることが考えられる。このような監視機関において上記故意の攻撃を避けるために、電子透かし方式や鍵の守秘性を保持することは重要である。

【００１１】

【発明が解決しようとする課題】

以上のように電子透かし方式にはその特徴に応じて種々の方式がある。また、電子透かしを用いてディジタルデータの不正コピー、及び不正出力を防止しようという企業、機関も多い。しかし、それらの企業、機関が独立に電子透かし方式を選択してデータに電子透かしを埋め込んだ場合、電子透かし方式の埋め込み処理と抽出処理は一対一に対応しており互換性がないために、以下のような問題が生じる。

【００１２】

①電子透かしの抽出処理を方式毎に行わなければならないので、１つの監視機関による統一的な検査が困難である。

②１つの監視機関によって統一的に検査を行う場合、その監視機関は全ての電子透かし抽出手法を準備しておく必要があり負荷が大きい。

③監視機関は、全ての抽出手法に対応する鍵を秘密かつ厳重に管理する必要がある。

④方式毎に監視機関をもつとした場合、埋め込まれた透かしが抽出できなかったとき、他の方式による透かしが入っているのか、透かしが攻撃によって壊されたのか判定できない。

尚、ここで１つの監視機関とは、物理的に１つという意味ではなく、標準化や国等によって定められた組織的又は方式的に１つの体制を指す。

【００１３】

本発明は上記の問題点に鑑みてなされたものであり、種々の電子透かし方式に対して効率的に著作物の保護等を実現することを目的としている。

【００１４】

【課題を解決するための手段】

上記の目的を達成するために、本発明による情報処理システムにおいては、複数の情報処理装置がネットワーク上に接続された情報処理システムにおいて、上記複数の情報処理装置のうちの少なくとも一つの情報処理装置に、入力情報に対して第１の付加情報を第１の付加方法により耐性強く付加する第１の付加手段と、上記入力情報に対して第２の付加情報を第２の付加方法により付加する第２の付加手段とを設けている。

【００１５】

また、本発明による他の情報処理システムにおいては、複数の情報処理装置がネットワーク上に接続された情報処理システムにおいて、上記複数の情報処理装置のうちの少なくとも一つの情報処理装置に、入力情報から第１の付加情報を第１の抽出方法により抽出する第１の抽出手段と、上記抽出された第１の付加情報から第２の抽出方法を特定し、この第２の抽出方法により上記入力情報から第２の付加情報を抽出する第２の抽出手段とを設けている。

【００１６】

また、本発明による情報処理装置においては、入力情報に対して第１の付加情報を第１の付加方法により耐性強く付加する第１の付加手段と、上記入力情報に対して第２の付加情報を第２の付加方法により付加する第２の付加手段とを設けている。

【００１７】

また、本発明による他の情報処理装置においては、入力情報に対して第１の付加情報を第１の抽出方法により抽出する第１の抽出手段と、第２の付加情報を第２の抽出方法により抽出する第２の抽出手段とを設けている。

【００１８】

また、本発明による記憶媒体においては、入力情報に対して第１の付加情報を耐性強く付加する第１の付加処理と、上記入力情報に対して第２の付加情報を付加する第２の付加処理とを実行するためのプログラムを記憶している。

【００１９】

また、本発明による他の記憶媒体においては、入力情報から第１の付加情報を抽出する第１の抽出処理と、上記抽出された第１の付加情報から抽出方法を特定

する特定処理と、上記特定された抽出方法により上記入力情報から第２の付加情報を抽出する第２の抽出処理とを実行するためのプログラムを記憶している。

【００２０】

【発明の実施の形態】

（第１の実施の形態）

図１は、本発明の第１の実施の形態による情報処理システムにおける電子透かしの埋め込みに関する部分を示したものである。特に、各監視機関独自の電子透かし方式と共通の電子透かし方式とをもつシステムを示したものである。ここで、共通の電子透かし方式とは、標準化又は関係する機関間で定められた電子透かし方式であり、その特徴は後述する。

【００２１】

図１において、１０１～１０４は異なる独自の電子透かし方式を用いて埋め込み処理を行う機関を示す。また、各機関１０１～１０４における各１０５は、定められた共通の電子透かし方式による埋め込み処理を行う共通透かし埋込装置であり、１０６～１０９は、各機関１０１～１０４毎に定めた独自の電子透かし方式による埋め込み処理を行うＡ～Ｄ透かし埋込装置である。１１０は各機関をつなぐネットワークであり、図示はしないが各機関１０１～１０４はこのネットワーク１１０に接続する通信手段を有している。

【００２２】

共通透かし埋込装置１０５で行われる共通の電子透かし方式は、以下の特徴をもつものとする。

（１）共通の電子透かしは、比較的少ない情報量で耐性の強い電子透かしを実現する。

（２）共通の電子透かしは、鍵なし又は共通の鍵によって電子透かしを抽出できる。

（３）共通の電子透かしは、少なくとも各電子透かし方式又はそれを用いて埋め込みを行った機関を特定する情報を埋め込む。

（４）共通の電子透かしは、各機関の電子透かし埋め込みに対する耐性をもつ。

【００２３】

上記の特徴をもつ電子透かしとしては種々の方式が考えられるが、耐性の強さをもつ一例として以下の方式を示す。

著作物である入力データを静止画像とした場合、その静止画の画像データを８×８画素のブロックに分割し、そのブロック毎にＤＣＴ（Ｄｉｓｃｒｅａｔｅ Ｃｏｓｉｎｅ Ｔｒａｎｓｆｏｒｍ：離散的コサイン変換）を行う。以下、そのＤＣＴしたブロックをＤＣＴ係数ブロック、ＤＣＴ係数ブロックの１係数をＤＣＴ係数、１枚の画像のＤＣＴ係数ブロックの集合をＤＣＴ係数ブロック群と呼ぶものとする。

【００２４】

図７（ａ）は上記透かし埋込装置を示し、図７（ｂ）は上記透かし抽出装置を示す。

（ａ）の透かし埋込装置において、入力画像ｘを画像変換器７０１によりＤＣＴ変換し、その出力であるＤＣＴ係数ブロック群を電子透かし埋め込み器７０２の入力として用いる。電子透かし埋め込み器７０２では、入力されたＤＣＴ係数ブロック群の中で、埋め込むＤＣＴ係数ブロックを１つ選択し、そのＤＣＴ係数ブロック中の１つのＤＣＴ係数を量子化することによって、１ビットの埋め込みビットを埋め込む。

この時の、量子化ステップの大きさが埋め込みの強度を決定し、その量子化ステップの大きさと選択したＤＣＴ係数の位置が鍵情報に対応する。

【００２５】

例として、座標ｕ，ｖの位置にあるＤＣＴ係数の値をｓ｛ｕ，ｖ｝、量子化ステップをｈと表わし、以下に示すような規則により、電子透かしビットの０又は１を埋め込む。

$a \cdot h < s\{u, v\} \leqq (a+1) \cdot h$ ――― （１）

となるａを求める。

【００２６】

埋め込みビット＝０の時　ｃ｛ｕ，ｖ｝＝ｂ・ｈ＋ｈ／２（ｂはａ又はａ＋１の偶数の方）――― （２）

埋め込みビット＝１の時　ｃ｛ｕ，ｖ｝＝ｂ・ｈ＋ｈ／２（ｂはａ又はａ＋１の奇数の方）――――（３）

となる操作を行い、ｃ｛ｕ，ｖ｝を埋め込み後の係数とする。

【００２７】

最後に、そのブロック群を逆変換器７０３を用いてＩＤＣＴ（Ｉｎｖｅｒｓｅ ＤＣＴ：逆ＤＣＴ）を行って、８×８画素のブロックに戻し、それを再構成する。これによって、電子透かしが埋め込まれた画像ｙが得られる。

【００２８】

電子透かしの抽出を行う場合は、図７（ｂ）の透かし抽出装置において、上記画像ｙを上記画像変換器７０１に入力して、同様のＤＣＴをしたＤＣＴ係数ブロック群から電子透かし抽出器７０５により、鍵情報を用いて埋め込んだＤＣＴ係数を選択し、

ｂ・ｈ＜ｃ｛ｕ，ｖ｝≦（ｂ＋１）・ｈ――――（４）

となるｂを求め、ｂが偶数ならば埋め込みビットは０と判断し、奇数ならば１と判断する。

【００２９】

この埋め込み方式において耐性を強化するには以下の手法が考えられる。

ＤＣＴ係数ブロックの中から埋め込みを行う１つのＤＣＴ係数を選択するときに、低周波成分を表わすＤＣＴ係数を選べば耐性を強くすることができる。これは、高周波成分が画像圧縮や種々のフィルタリング処理によって失われやすいのに対して、低周波成分は失われにくいためである。

【００３０】

また、上記の埋め込み方式では選択するＤＣＴ係数ブロック、及び埋め込むＤＣＴ係数を１つとして説明したが、その数を増すことによっても耐性を強くすることができる。これは、１ビットに対して１つのＤＣＴ係数に埋め込んだのみであると、画像圧縮や種々のフィルタリング処理によってその値が失われる可能性が大きいが、複数のＤＣＴ係数に同じビットを埋め込んでおけば、その大半が失われる可能性が少なくなるためである。

【００３１】

また、埋め込むビット自体を誤り訂正符号化することによっても耐性を強くすることができる。これは、埋め込みビットのいくつかが失われても誤り訂正符号によって復元されるためである。ここで、用いる誤り訂正符号の訂正能力が高ければ高いほど耐性が強くなるのは明らかである。ただし、これらの手法は耐性を強くするが、画像の低周波成分を変化させたり、多くのビットを埋め込むために画像の品質が劣化する。また、多くのＤＣＴ係数を用いて同じビットを埋め込むために、埋め込めるビットは少なくなることが多い。また、逆の操作を行えば、耐性は弱くなるが、画質が良く、埋め込める情報量も多い電子透かし手法が実現できる。

【００３２】

以上のような耐性を強化する手法は、ＤＣＴを用いる手法に限らず、ウェーブレット変換やフーリエ変換を用いる手法や、直接画素の輝度値などを操作する手法に対しても同じ傾向をもつと言える。

【００３３】

次に、図１を参照して埋め込み手順を説明する。ここでは、共通の電子透かし方式によって埋め込む情報を、簡単のために００、０１、１０、１１とし、各機関１０１～１０４を特定する２ビットの情報とするが、他の情報を設定することもできることは明らかである。

【００３４】

各機関１０１～１０４は、配布されるデータに対して上記（１）～（４）の特徴をもつ耐性の強い共通透かし埋込装置１０５を用いて自機関に対応するビットを埋め込む。その後に各機関独自のＡ～Ｄ透かし埋込装置１０６～１０９を用いて他の情報を埋め込む。また、ある機関の電子透かし方式と共通の電子透かし方式とが干渉し合わない、即ち、電子透かし埋め込み処理によって共通の電子透かし情報に影響を与えない手法であれば、埋め込み順序は逆にすることもできる。また、各機関毎に埋め込む情報は異なっていても良いし、同じ情報でも良い。各機関毎に埋め込む情報としては、著作権情報や利用者情報及び識別情報など種々の情報であることが考えられる。

【００３５】

図２は第１の実施の形態のうちの電子透かしの抽出に関する部分を示す。

図２において、２００は統一的な１つの監視機関であり、２０１～２０４は図１の各機関１０１～１０４に対応する各機関毎の電子透かし監視機関である。統一監視機関２００は、図１の共通透かし埋込装置１０５に対応する共通透かし抽出装置２０５を有し、各機関２０１～２０４は図１のＡ～Ｄ透かし埋込装置１０６～１０９に対応する各電子透かし方式によるＡ～Ｄ透かし抽出装置２０６～２０９を有している。２１０は各機関２０１～２０４をつなぐネットワークであり、図示はしないが各機関２０１～２０４は、このネットワーク２１０に接続する通信手段を有している。このネットワーク２１０は図１のネットワーク１１０と同じものでもよい。

【００３６】

以下、図２における電子透かしの抽出手順を説明する。

統一的な機関２００は、ネットワーク２１０で流通又は利用されているデータの監視を行う。ネットワーク上で不正コピーと思われるデータが発見又は通報された場合は、共通透かし抽出器２０５を用いて共通の電子透かしによる埋め込み情報を抽出する。これによって、埋め込みを行った機関又は方式を特定し、そのデータを特定された機関に送る。

【００３７】

データを送られた機関は、各機関独自の電子透かし方式のＡ～Ｄ透かし抽出装置２０６～２０９を用いて埋め込んだ種々の情報を抽出する。

【００３８】

本実施の形態によれば、異なる電子方式が混在して用いられるシステムにおいても、各監視機関は多くの方式による電子透かしの埋込部や抽出部を準備することなく、自分の電子透かし方式による埋込部や抽出部のみを管理すればよく、効率的に不正コピーの監視を実現することができる。

【００３９】

また、透かしが発見できなかった場合の安全性も以下の理由により向上できる。即ち、埋め込んだ透かし情報が発見できなかった場合、そのデータには始めから透かし情報がなかったのか、他の方式によって透かしが埋め込まれているのか

、透かし情報が攻撃によって破壊されたのかを区別することは困難である。しかし、共通の電子透かし方式は耐性が強いので、透かし情報を攻撃によって破壊することは困難である。

【００４０】

従って、最初の手順によって共通の電子透かしによる透かし情報が抽出された場合、始めから透かし情報が入っていなかった可能性は排除される。次に、各機関独自の電子透かし方式は任意であるが、詳細情報を埋め込む場合、埋め込む情報量が多くなり品質劣化の抑制を重視した比較的耐性の弱い電子透かし方式となる場合が多い。従って、共通の電子透かし方式による透かし情報の抽出後に各機関独自の電子透かし方式による透かし情報が抽出できない場合は、攻撃による電子透かし情報の破壊であると言える。

【００４１】

よって、このシステムによって各機関が単独に独白電子透かし方式を用いるよりも全体的な安全性が向上していることが言える。

尚、本実施の形態では４つの機関からなる例について説明したが、任意の数の機関に対しても同様に実施できることは明らかである。

【００４２】

（第２の実施の形態）

図３は、本発明の第２の実施の形態による情報処理システムにおける電子透かしの埋め込みに関する部分を示す。本実施の形態は、共通透かし埋込装置１０５による埋め込みを、共通埋め込み機関３００のみが行う場合である。

３０１～３０４は、図１の各機関１０１～１０４からそれぞれ共通透かし埋込装置１０５を除いた独自の電子透かし方式によるＡ～Ｄ透かし埋込装置１０６～１０９のみをもつ各機関であり、１１０はネットワークである。

【００４３】

尚、共通埋め込み機関３００としては、音楽著作物に対するＪＡＳＲＡＣのような統一的な著作権管理機関が考えられ、各機関３０１～３０４としては、共通埋め込み機関３００によって管理されている著作物をユーザに販売する販売店のような形態が考えられるが、本実施の形態で特定するものではなく、共通で耐性

の強い電子透かし方式と各機関独自の電子透かし方式とを用途に応じて使い分ける手法は全て本発明に含まれる。

【００４４】

この場合は各機関３０１～３０４（個々の著作者を含む）は、著作物を機関３００に登録し、共通透かし埋込装置１０５による埋め込みを依頼する。機関３００は共通の電子透かし方式によって所定の情報を埋め込み、各機関３０１～３０４に返信する。各機関３０１～３０４は、それぞれ独自の電子透かし方式によるＡ～Ｄ埋込装置１０６～１０９を用いて種々の情報を埋め込む。

【００４５】

本実施の形態の第１の実施の形態に対する利点は次の通りである。

第１の実施の形態では、各機関が共通の電子透かし方式による埋め込みを行うために、共通の電子透かし方式、及びその鍵は各機関に公開されている必要がある。安全性のためには共通の電子透かし方式及び鍵は秘密にした方が良いが、各機関の内の１つでもその秘密を守れなければ全体の安全性が保持できない。しかし、本実施の形態では、共通の電子透かし方式を各機関３０１～３０４に公開する必要がないので安全性が向上する。

【００４６】

また、第１の実施の形態と融合した形態も考えられる。例えば、図３において機関３０１と３０２は第１の実施の形態と同様に共通透かし埋込装置１０５をもつものとする。この場合、共通透かし埋込装置１０５を持たない機関３０３と３０４は本実施の形態と同様の処理を行うが、共通透かし埋込装置１０５をもつ機関１０１と１０２は共通の電子透かし方式による所定情報の埋め込みを第１の実施の形態のように自機関内で行うことができる。

【００４７】

図４は第２の実施形態による情報処理システムにおける電子透かしの抽出に関する部分を示す。

図４において、４００は統一的な１つの監視機関であり、共通透かし埋込装置１０５に対応する共通埋込装置２０５と、各機関独自の電子透かし方式によるＡ～Ｄ埋込装置１０６～１０９に対応するＡ～Ｄ抽出装置２０６～２０９を有する

。２１０はネットワークである。尚、図示していないが図１又は図３の各機関１０１～１０４又は３０１～３０４等がネットワーク２１０に接続されているものとする。

【００４８】

以下、図４における電子透かしの抽出手順を説明する。

機関４００はネットワーク２１０で流通又は利用されているデータの監視を行う。ネットワーク上で不正コピーと思われるデータが発見又は通報された場合は、共通透かし埋込装置２０５を用いて共通の電子透かしによる埋め込み情報を抽出する。これによって、埋め込みを行った機関又は方式を特定する。次に、特定された機関独自の電子透かし方式の抽出装置を用いて埋め込んだ種々の情報を抽出する。

【００４９】

本実施の形態によるシステムでは、１つの統一的な監視機関だけで不正コピーの監視が可能である。このような統一的な監視機関は、各機関独自の電子透かし方式が有限であれば実現可能である。また、共通の電子透かし方式によって各機関独自の電子透かし方式が特定されるので、試行錯誤的に各機関独自の電子透かし方式を試す必要がなく効率的である。

【００５０】

ただし、統一監視機関は始めから全ての各機関独自の電子透かし方式を準備している必要はなく、共通の電子透かし方式による透かし情報によって埋め込み機関が特定されたときに、その機関に連絡して各機関独自の電子透かし方式の抽出手段及び鍵などを提供してもらうこともできる。

【００５１】

（第３の実施の形態）

図５は図１及び図３に対応する電子透かしの抽出に関する部分を示す。

図５において、５０１～５０４は共通透かし埋込装置１０５に対応する共通透かし抽出装置２０５と、各機関独自の電子透かし方式によるＡ～Ｄ埋込装置１０６～１０９に対応するＡ～Ｄ抽出装置２０６～２０９を各々有する。

【００５２】

以下、図５における電子透かしの抽出手順を説明する。

各機関５０１～５０４はネットワーク２１０で流通又は利用されているデータの監視を行う。ネットワーク上で不正コピーと思われるデータが発見又は通報された場合は、共通透かし抽出装置２０５を用いて共通の電子透かしによる埋め込み情報を抽出する。これによって、埋め込みを行った機関又は方式を特定し、自機関の方式と特定された場合は、自機関独自の透かし抽出装置により抽出を行う。他機関である場合は、状況に応じて通報又は破棄等の処理を行う。

【００５３】

本実施の形態によるシステムでは、統一的な監視機関をもたずに不正コピーの監視が可能である。このシステムは図１及び図３のどちらの埋め込みシステムにも対応可能である。また、図２、図４も図１及び図３のどちらの埋め込みシステムにも対応可能であることは明らかである。

【００５４】

また、図２、図４、図５を融合した形態も考えられる。例えば、第１の実施の形態の図２において、機関２００は第２の実施の形態の機関３００のように全てのＡ～Ｄ透かし抽出装置をもち、機関２０１と２０２は第３の実施の形態と同様に共通透かし抽出装置２０５をもつものとする。この場合、共通透かし抽出装置２０５をもたない機関２０３と２０４は第１の実施の形態と同様の処理を行うが、共通透かし抽出装置２０５を持つ機関３００及び２０１と２０２は共通透かし抽出装置による透かし情報の抽出を第２、３の実施の形態のように自機関内で行うことができる。

以上を含めて、共通で耐性の強い電子透かし方式と各機関独自の電子透かし方式を用途に応じて使い分ける手法は全て本発明に含まれる。

【００５５】

（第４の実施の形態）

図１、図３の埋め込みシステムにおいて、各機関はその埋込装置に対応する抽出装置を有し、埋め込み前に透かし情報の抽出検査を行う形態も可能である。

本実施の形態としては、上述の各実施の形態及びその組み合わせが考えられるが、ここでは図３に示した形態を例に図６を参照して説明を行う。

図６において、６００は共通の埋め込み機関であり、共通透かし埋込装置１０５と、それに対応する共通透かし抽出装置２０５を有する。６０１～６０４は各機関独自の電子透かし方式によるＡ～Ｄ透かし埋込装置１０６～１０９と、それに対応するＡ～Ｄ透かし抽出装置２０６～２０９を有する機関である。

【００５６】

各機関６０１～６０４（個々の著作者を含む）は著作物を機関６００に登録し、共通透かし埋込装置１０５による埋め込みを依頼する。機関６００は、共通透かし埋込装置１０５を用いる前に、共通透かし抽出装置２０５を用いてその著作物が不正コピーでないことを確認する。例えば、共通透かし抽出装置２０５によってその著作物に既に共通の電子透かしが埋め込まれていることが分かった場合は、依頼元又は透かし情報によって特定された機関に確認を行う。問題がなければ共通透かし埋込装置１０５によって所定の情報を埋め込み依頼元に返信する。依頼元は各機関独自の埋込装置１０６～１０９を用いて種々の情報を埋め込む。

【００５７】

本実施の形態によるシステムによれば、依頼者の不正申告による電子透かしの上書きなどを防ぐことができる。また、埋め込み機関と抽出機関を同じにして効率的なシステムを実現することもできる。

【００５８】

次に、本発明の他の実施の形態としての記憶媒体について説明する。

本発明は上記各実施の形態で説明したシステムや装置を組み合わせて行う場合のみに限定されるものではなく、上記システム又は装置内のコンピュータ（ＣＰＵあるいはＭＰＵ）に、上記各実施の形態を実現するためのソフトウエアのプログラムコードを供給し、このプログラムコードに従って上記システムあるいは装置のコンピュータが上記各種デバイスを動作させることにより、上記各実施の形態を実現する場合も本発明の範疇に含まれる。

【００５９】

またこの場合、上記ソフトウエアのプログラムコード自体が上記各実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、具体的には上記プログラムコード

を格納した記憶媒体は本発明の範疇に含まれる。

【００６０】

このようなプログラムコードを格納する記憶媒体としては、例えばＲＯＭ、ＲＡＭ等の半導体メモリ、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性メモリカード、を用いることができる。

【００６１】

また、上記コンピュータが、供給されたプログラムコードのみに従って各種デバイスを制御することにより、上記各実施の形態の機能が実現される場合だけではなく、上記プログラムコードがコンピュータ上で稼働しているＯＳ（オペレーティングシステム）、あるいは他のアプリケーションソフト等と共同して上記各実施の形態が実現される場合にも、かかるプログラムコードは本発明の範疇に含まれる。

【００６２】

さらに、プログラムがコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能格納ユニットに備わるＣＰＵ等が実際の処理の一部又は全部を行い、その処理によって上記各実施の形態が実現される場合も本発明の範疇に含まれる。

【００６３】

【発明の効果】

以上説明した通り、本発明によれば、異なる電子方式が混在して用いられるシステムにおいても、監視機関は多くの電子透かしの埋込装置や抽出装置を準備することなく、効率的に不正コピーを監視することができる。また、電子透かしが発見できなかった場合の安全性も各電子透かし方式単独に用いるよりも向上させることができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態による情報処理システムにおける電子透かしの埋め込みに関する部分を示すブロック図である。

【図２】

本発明の第１の実施の形態による情報処理システムにおける電子透かしの抽出に関する部分を示すブロック図である。

【図３】

本発明の第２の実施の形態による情報処理システムにおける電子透かしの埋め込みに関する部分を示すブロック図である。

【図４】

本発明の第２の実施の形態による情報処理システムにおける電子透かしの抽出に関する部分を示すブロック図である。

【図５】

本発明の第３の実施の形態による情報処理システムにおける電子透かしの抽出に関する部分を示すブロック図である。

【図６】

本発明の第４の実施の形態による情報処理システムにおける電子透かしの埋め込みと抽出に関する部分を示すブロック図である。

【図７】

電子透かしの埋込装置及び抽出装置を示すブロック図である。

【符号の説明】

１０１～１０４　監視機関

１０６～１０９　Ａ～Ｄ透かし埋込装置

１１０　ネットワーク

２００　統一的な監視機関

２０４～２０４　監視機関

２０５　共通透かし抽出装置

２０６～２０９　Ａ～Ｄ透かし抽出装置

２１０　ネットワーク

３００　共通埋め込み機関

３０１～３０４　監視機関

４００　統一的な監視機関

５０１～５０４　監視機関

６００　共通埋め込み機関

６０１～６０４　監視機関

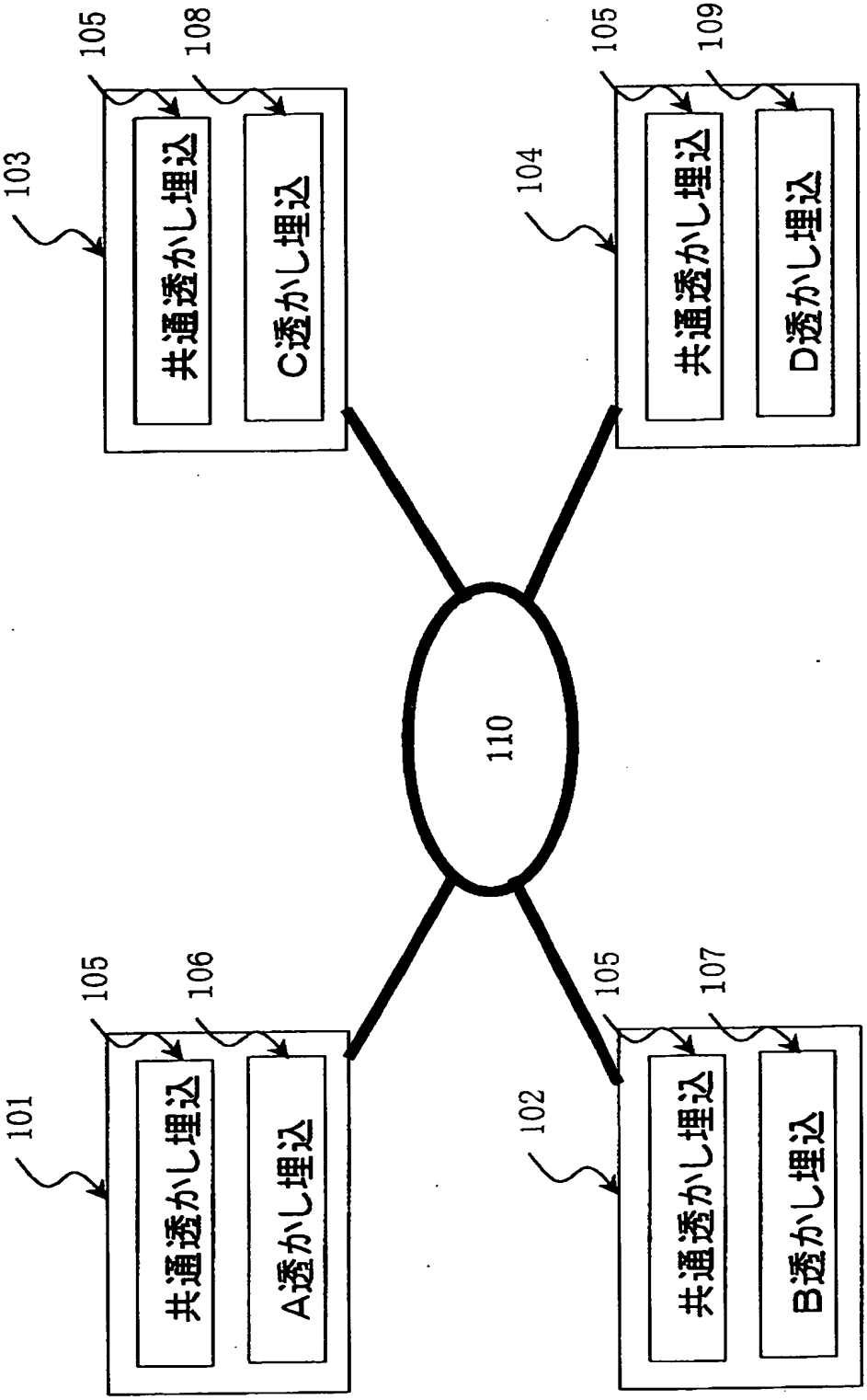
７０１　画像変換器

７０２　電子透かし埋め込み器

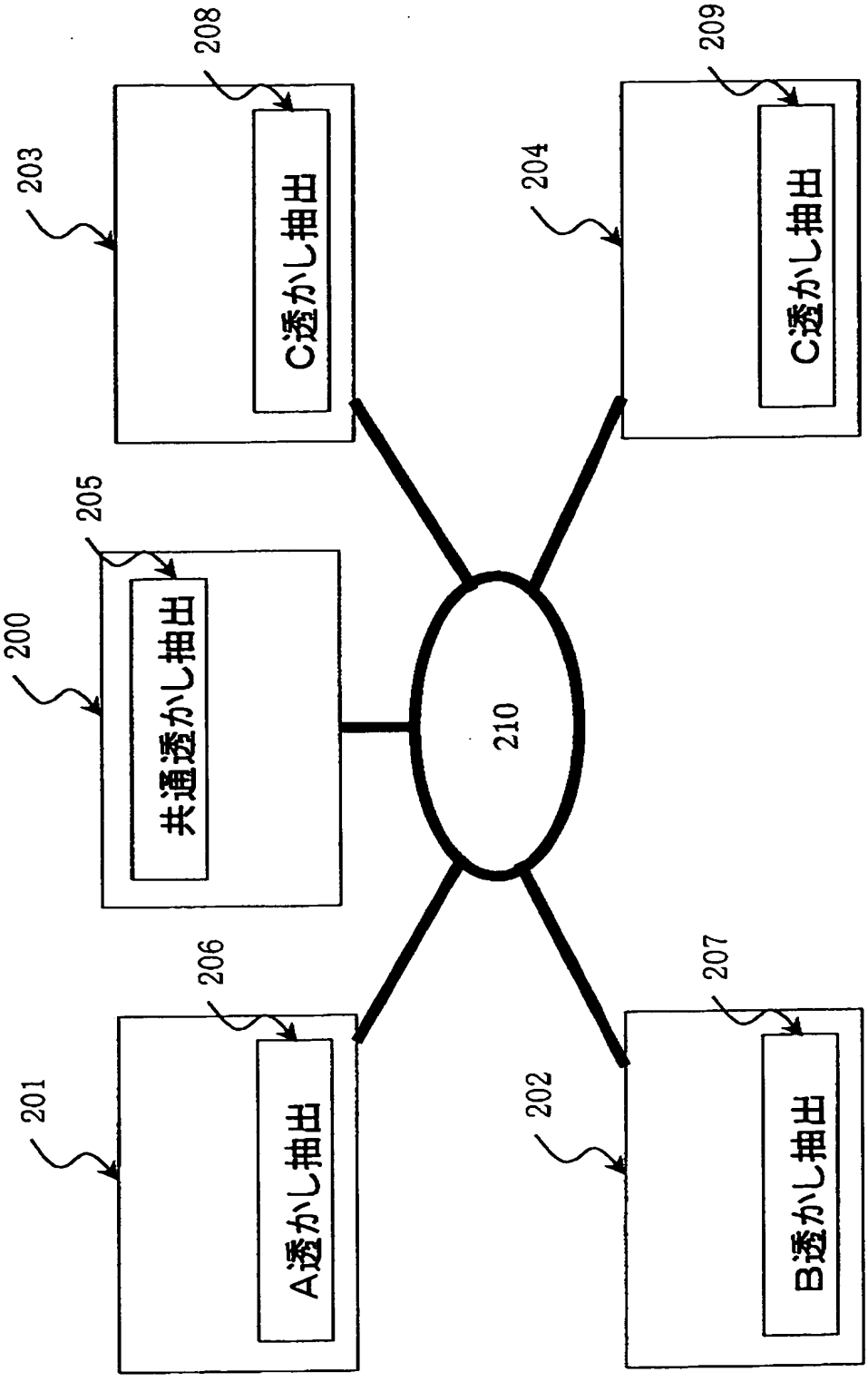
７０３　画像逆変換器

７０５　電子透かし抽出器

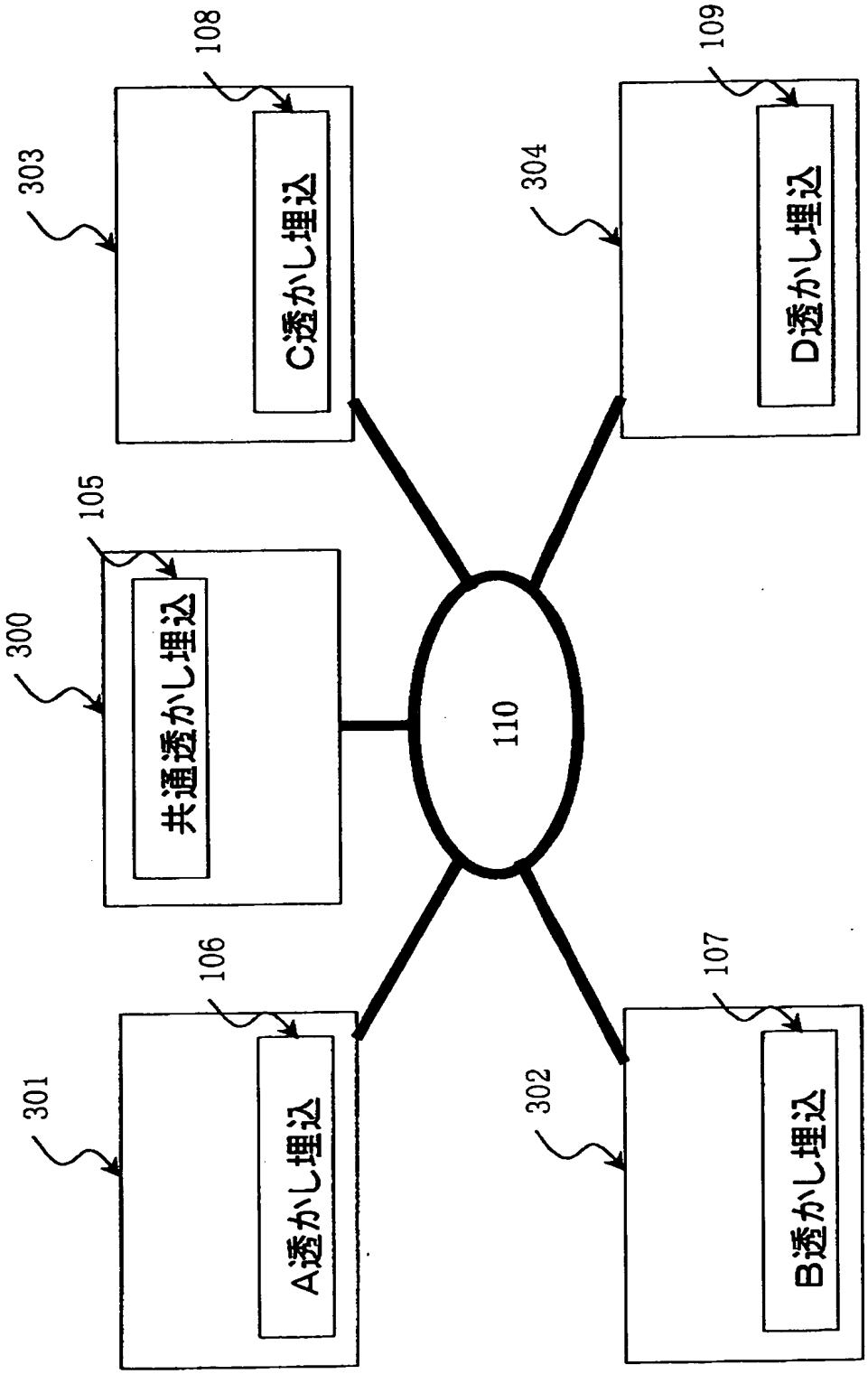
【図１】


101
102
103
104
105
106
107
108
109
110
共通透かし埋込
A透かし埋込
B透かし埋込
C透かし埋込
D透かし埋込

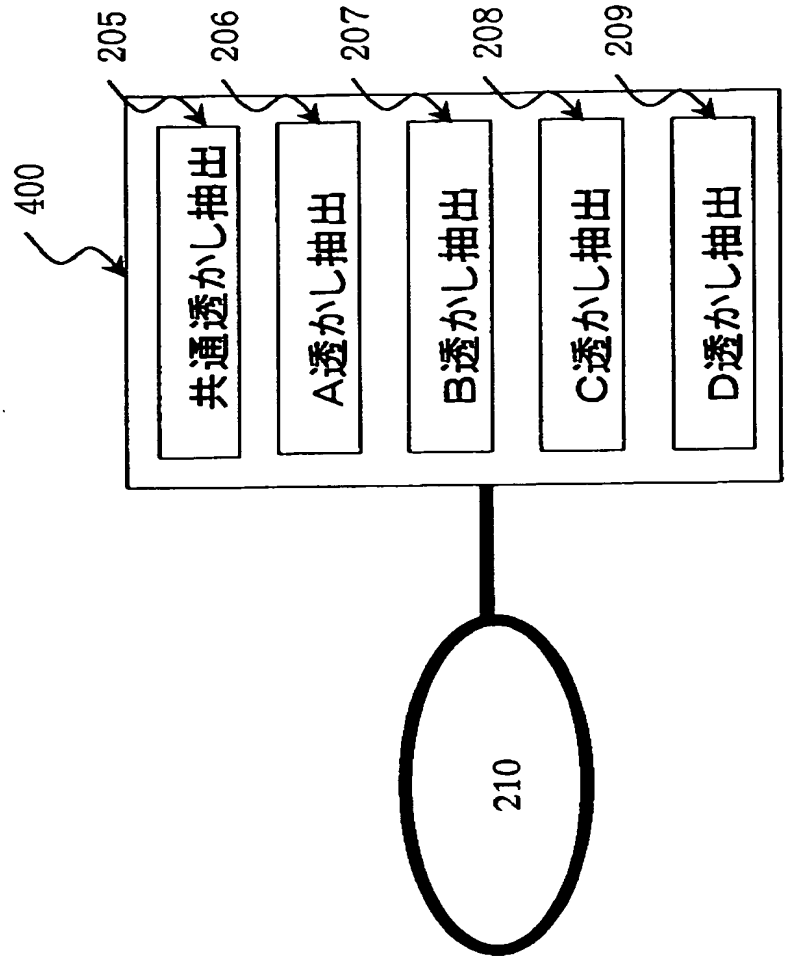
【図２】


208
209
203
C透かし抽出
204
C透かし抽出
205
200
共通透かし抽出
210
206
207
201
A透かし抽出
202
B透かし抽出

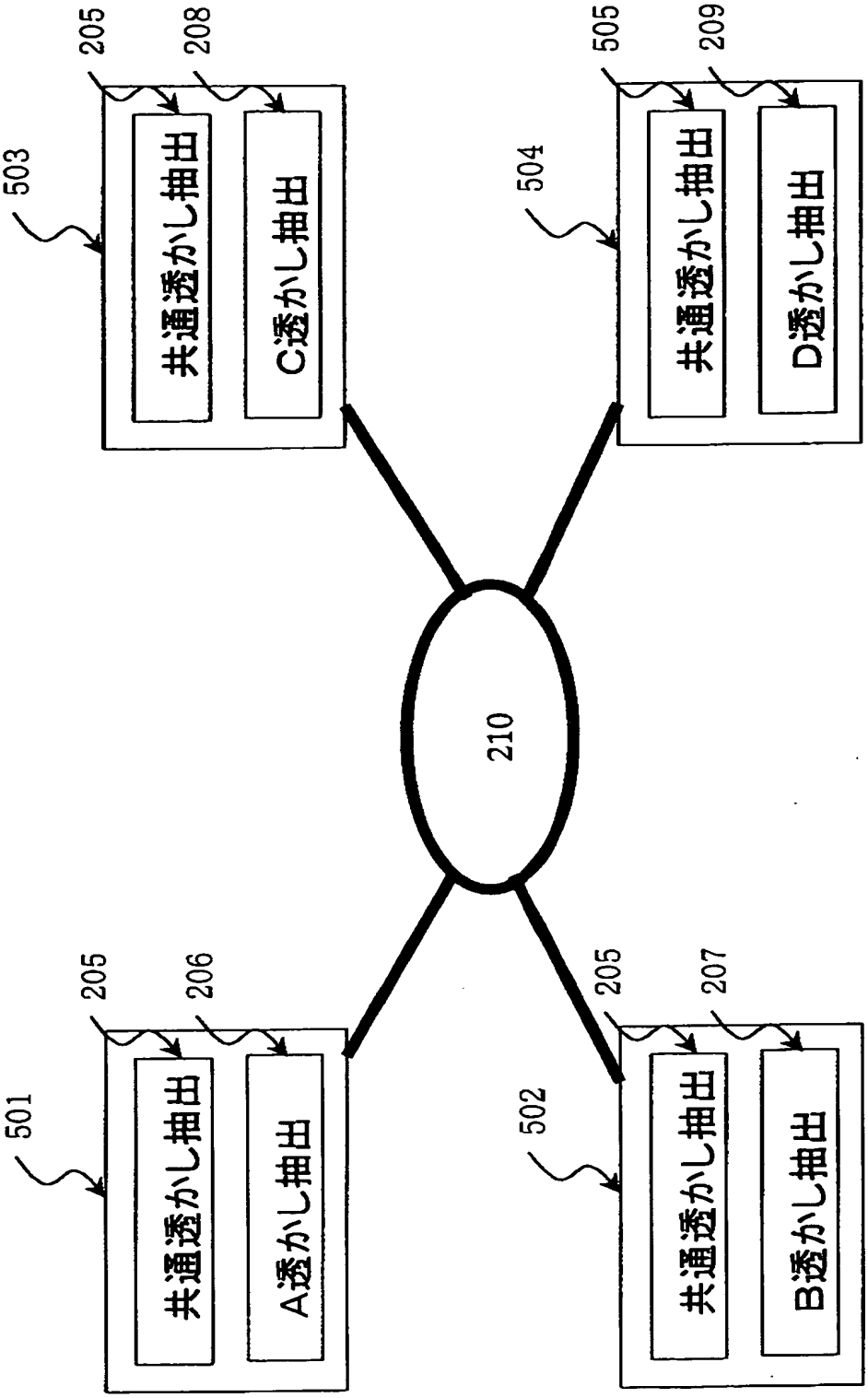
【図３】


108
C透かし埋込
303
109
D透かし埋込
304
105
共通透かし埋込
300
110
106
A透かし埋込
301
107
B透かし埋込
302

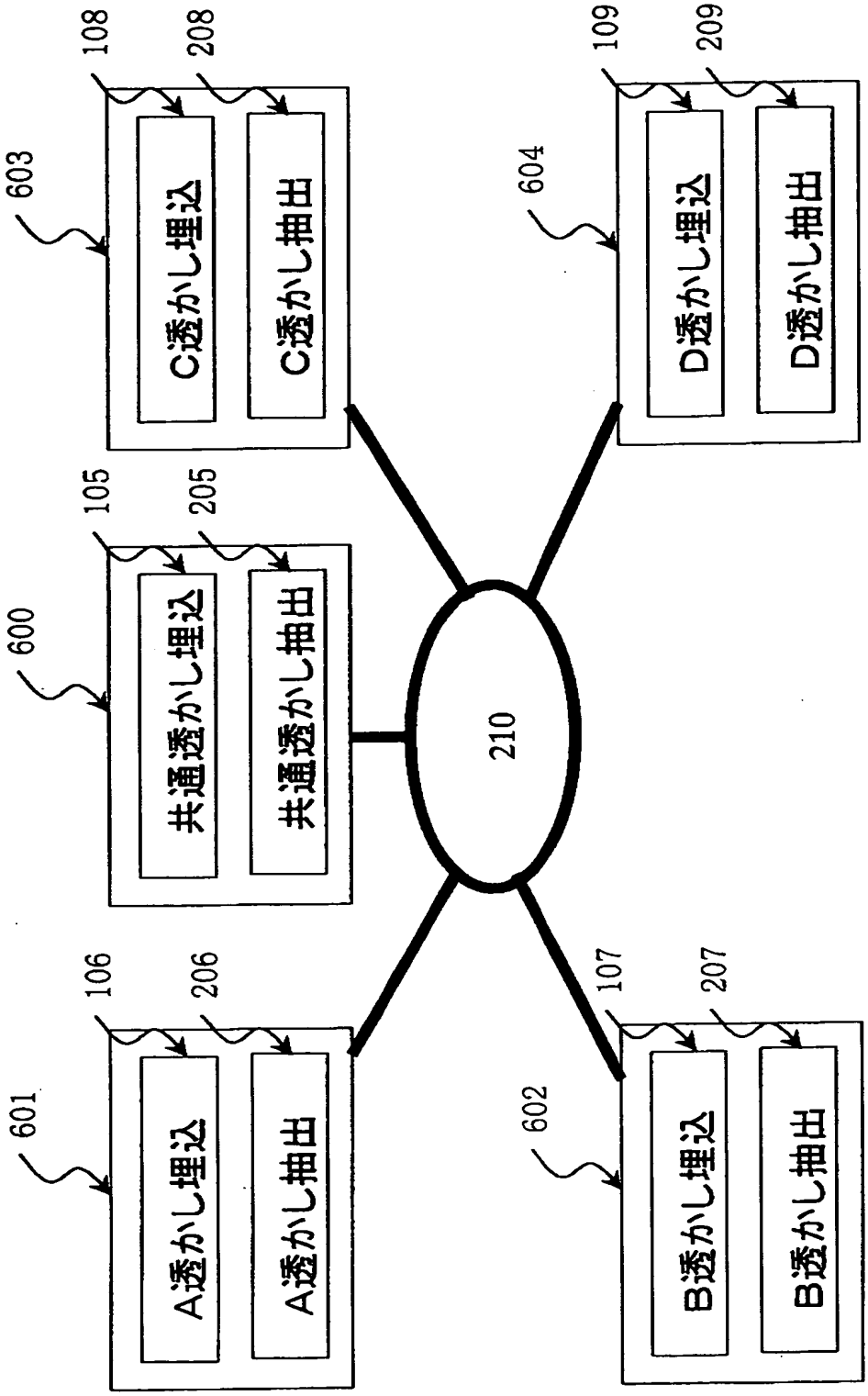
【図４】


205
206
207
208
209
400
共通透かし抽出
A透かし抽出
B透かし抽出
C透かし抽出
D透かし抽出
210

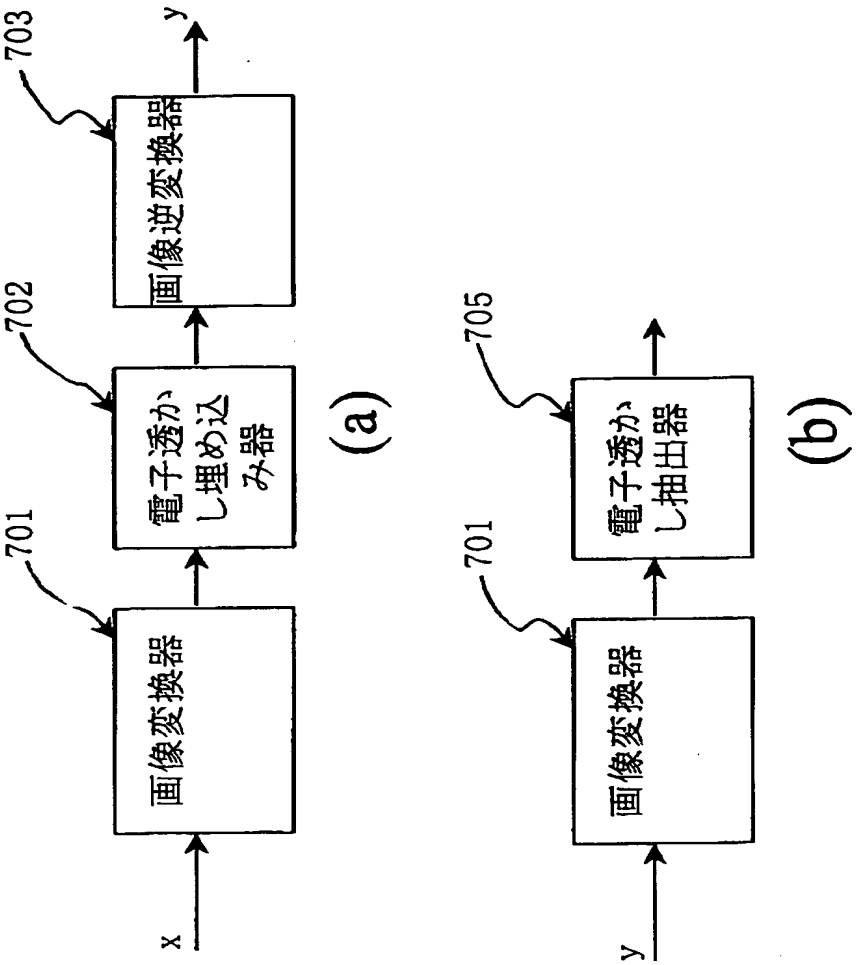
【図５】


205
208
503
共通透かし抽出
C透かし抽出
505
209
504
共通透かし抽出
D透かし抽出
210
205
206
501
共通透かし抽出
A透かし抽出
205
207
502
共通透かし抽出
B透かし抽出

【図６】


108
208
603
C透かし埋込
C透かし抽出
109
209
604
D透かし埋込
D透かし抽出
105
205
600
共通透かし埋込
共通透かし抽出
210
106
206
601
A透かし埋込
A透かし抽出
107
207
602
B透かし埋込
B透かし抽出

【図７】


703
y
画像逆変換器
702
電子透かし埋め込み器
701
画像変換器
x
(a)
705
電子透かし抽出器
701
画像変換器
y
(b)

【書類名】　　要約書

【要約】

【課題】　種々の電子透かし方式に対して効率的に著作権の保護等を行えるようにする。

【解決手段】　各監視機関１０１～１０４は、配布される入力情報に対して共通透かし埋込装置１０５を用いて自機関に対応する耐性の強い情報を電子透かしとして埋め込む。その後、各機関独自の電子透かし方式にるＡ～Ｄ透かし埋込装置１０６～１０９を用いて他の情報を埋め込む。また、所定の監視機関がネットワーク上で不正コピーデータを発見したとき、共通透かし抽出装置を用いて上記共通透かし埋込装置による埋め込み情報を抽出する。これにより埋め込みを行った機関が特定され、そのデータを特定された機関に送る。その機関は、各機関独自の抽出装置を用いて埋め込んだ種々の情報を抽出する。従って、各機関は多くの方式による埋込装置や抽出装置を設けることなく、自分の方式による埋込装置や抽出装置のみを管理すればよい。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００１００７〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社